csm-ace 2014

CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

Are the “bad guys” getting smarter?

Shaharil Abdul Malek

CTO

SCAN Associates Berhad

DISCLAIMER

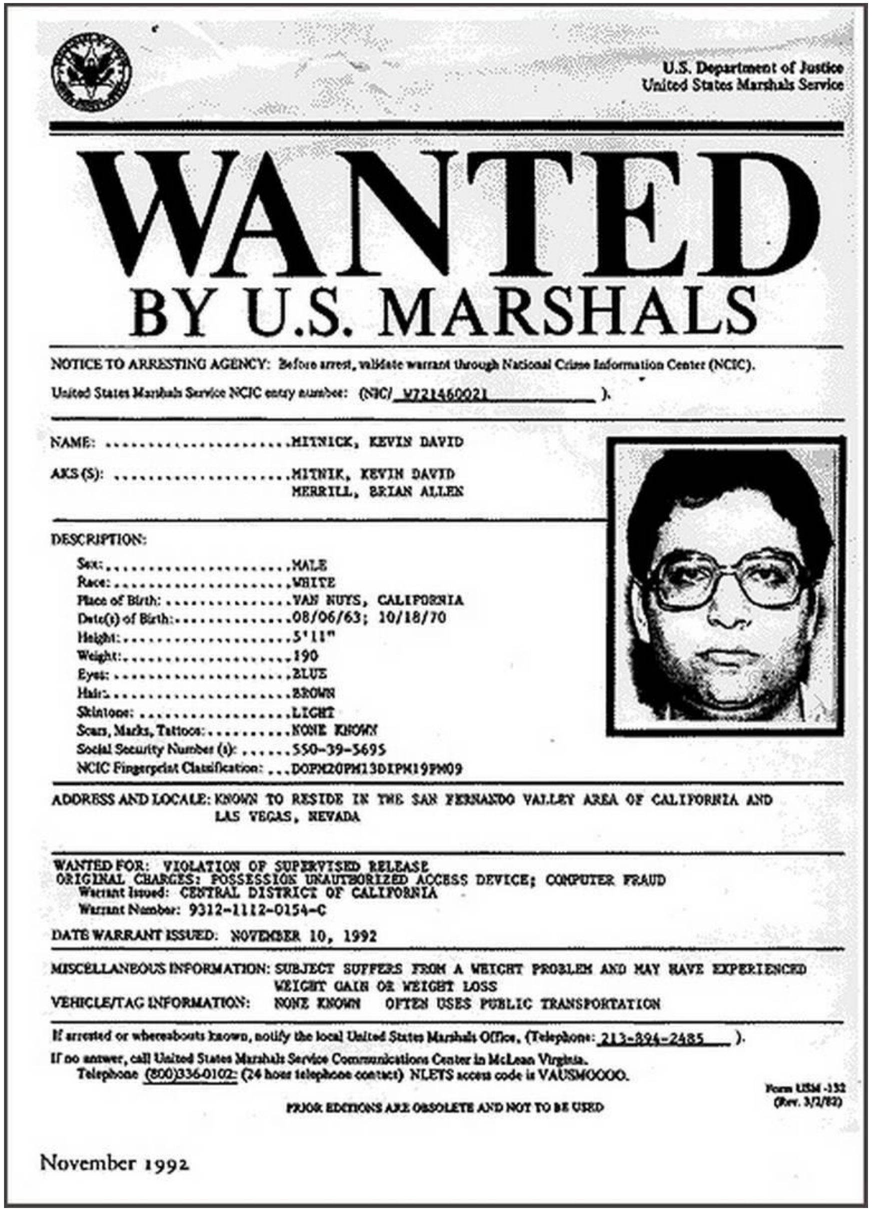
- Images are owned by their respective copyright owner.
- The opinion express during the presentation may not represent my current or future employer

Who are the bad guys??

Category

1. **Organized crime gang**
2. **State sponsored**
   - **Patriotism**
3. **Hacktivism**
4. Disgruntled staff / ex-contractor
5. Ex-BF/GF/H/W

Famous Cybercriminal



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex:......................MALE
Race:......................WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth:..............08/06/63; 10/18/70
Height:......................5'11"
Weight:......................190
Eyes: ....BLUE
Hair:......................BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos:..........NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND
LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED
WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSMOOOO.

Form USM-132
(Rev. 3/2/82)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

Famous Cybercriminal

Oleg Nikolaenko aka “King of SPAM”

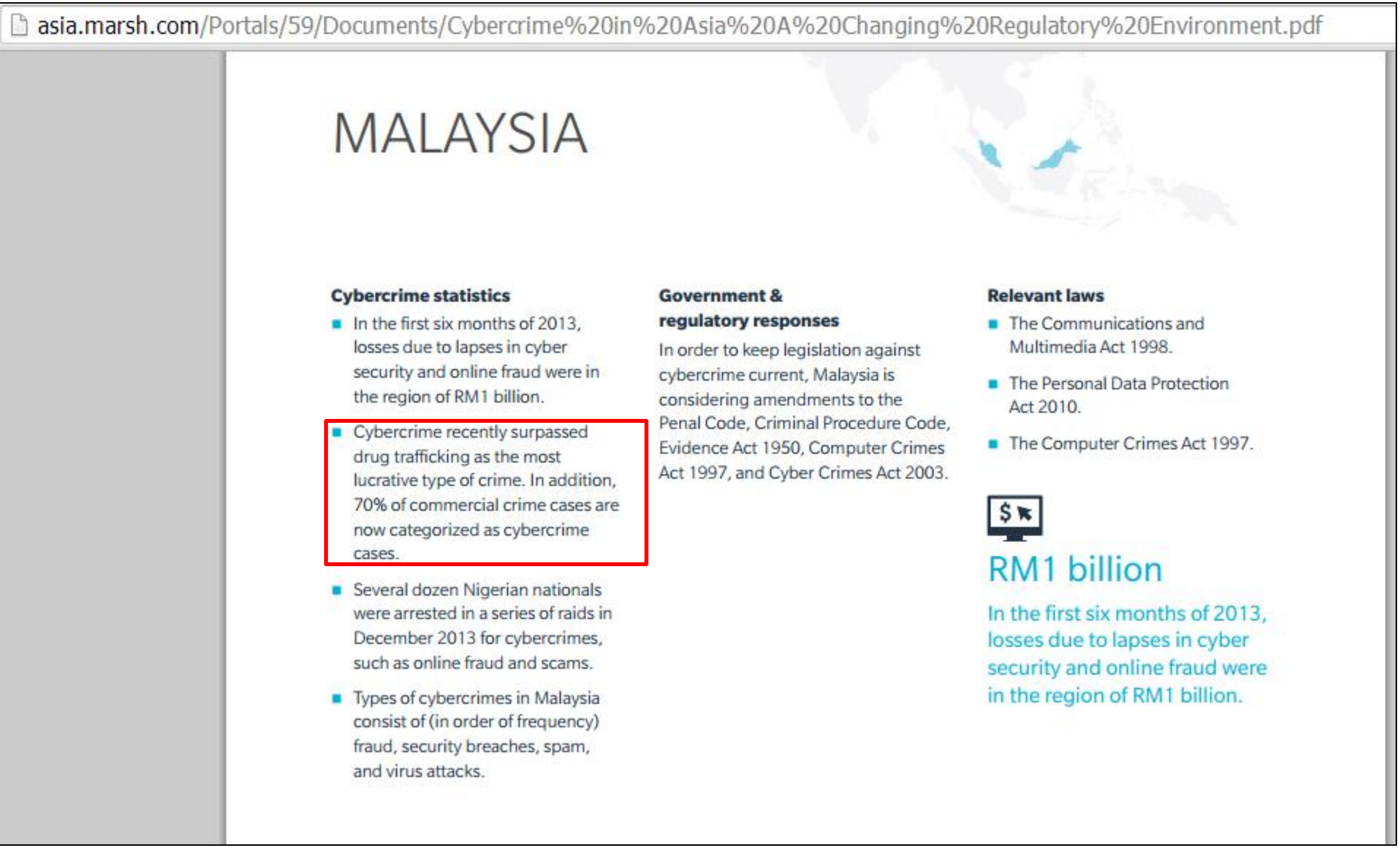
Estimated 1/3 worldwide SPAM

Mega-D botnet with 500k “zombies”

10 billion e-mails per day!

VIAGRA
CIALIS
100mg x 30 pills
only $139.00
20mg x 30 pills
only $139.00
WHEN YOU NEED IT NOW...
36-HOURS ERECTION POWER!!!
WISH TO BUY? GO TO WWW.PILLS10.COM

Malaysia



asia.marsh.com/Portals/59/Documents/Cybercrime%20in%20Asia%20A%20Changing%20Regulatory%20Environment.pdf

MALAYSIA

Cybercrime statistics

- In the first six months of 2013, losses due to lapses in cyber security and online fraud were in the region of RM1 billion.
- Cybercrime recently surpassed drug trafficking as the most lucrative type of crime. In addition, 70% of commercial crime cases are now categorized as cybercrime cases.
- Several dozen Nigerian nationals were arrested in a series of raids in December 2013 for cybercrimes, such as online fraud and scams.
- Types of cybercrimes in Malaysia consist of (in order of frequency) fraud, security breaches, spam, and virus attacks.

Government & regulatory responses

In order to keep legislation against cybercrime current, Malaysia is considering amendments to the Penal Code, Criminal Procedure Code, Evidence Act 1950, Computer Crimes Act 1997, and Cyber Crimes Act 2003.

Relevant laws

- The Communications and Multimedia Act 1998.
- The Personal Data Protection Act 2010.
- The Computer Crimes Act 1997.

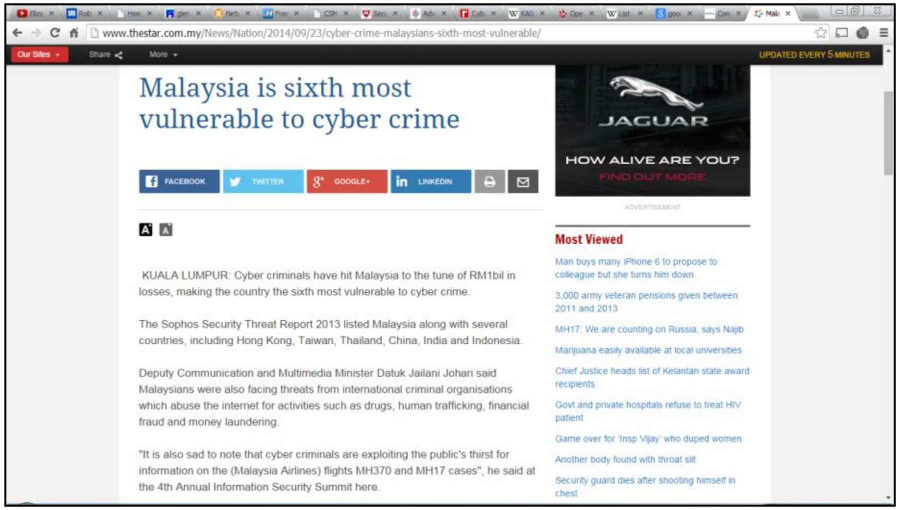
$

RM1 billion

In the first six months of 2013, losses due to lapses in cyber security and online fraud were in the region of RM1 billion.

Source: Cybercrime in Asia: A Changing Regulatory Environment Marsh LLC

23 Sept 2014:
Malaysia is sixth most vulnerable to cyber crime



Malaysia is sixth most vulnerable to cyber crime

KUALA LUMPUR: Cyber criminals have hit Malaysia to the tune of RM1bil in losses, making the country the sixth most vulnerable to cyber crime.

The Sophos Security Threat Report 2013 listed Malaysia along with several countries, including Hong Kong, Taiwan, Thailand, China, India and Indonesia.

Deputy Communication and Multimedia Minister Datuk Jailani Johari said Malaysians were also facing threats from international criminal organisations which abuse the internet for activities such as drugs, human trafficking, financial fraud and money laundering.

"It is also sad to note that cyber criminals are exploiting the public's thirst for information on the (Malaysia Airlines) flights MH370 and MH17 cases", he said at the 4th Annual Information Security Summit here.

Most Viewed

Man buys many iPhone 6 to propose to colleague but she turns him down

3,000 army veteran pensions given between 2011 and 2013

MH17: We are counting on Russia, says Najib

Marijuana easily available at local universities

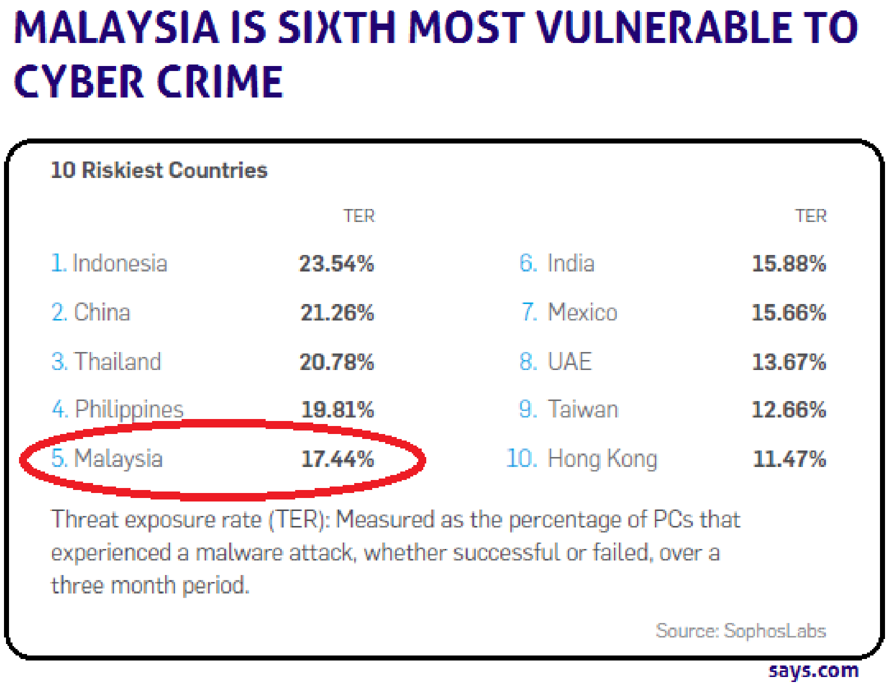
Chief Justice heads list of Kelantan state award recipients

Govt and private hospitals refuse to treat HIV patient

Game over for 'Insp Vijay' who duped women

Another body found with throat slit

Security guard dies after shooting himself in chest



MALAYSIA IS SIXTH MOST VULNERABLE TO CYBER CRIME

10 Riskiest Countries

	TER		TER
1. Indonesia	**23.54%**	6. India	**15.88%**
2. China	**21.26%**	7. Mexico	**15.66%**
3. Thailand	**20.78%**	8. UAE	**13.67%**
4. Philippines	**19.81%**	9. Taiwan	**12.66%**
5. Malaysia	**17.44%**	10. Hong Kong	**11.47%**

Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period.

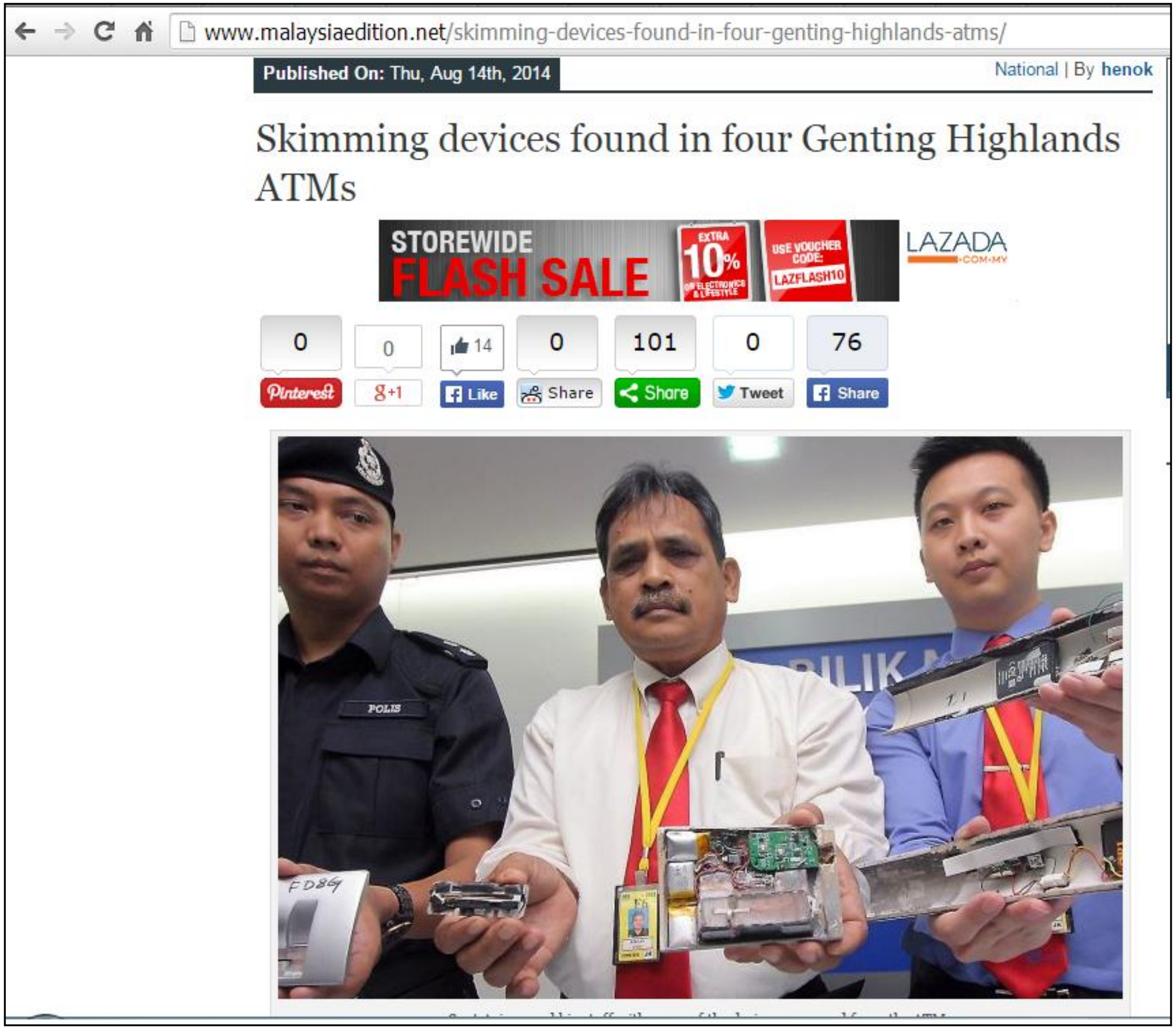
Source: SophosLabs

says.com

- http://www.thestar.com.my/News/Nation/2014/09/23/cyber-crime-malaysians-sixth-most-vulnerable/

The new wave?

ATM Skimmer



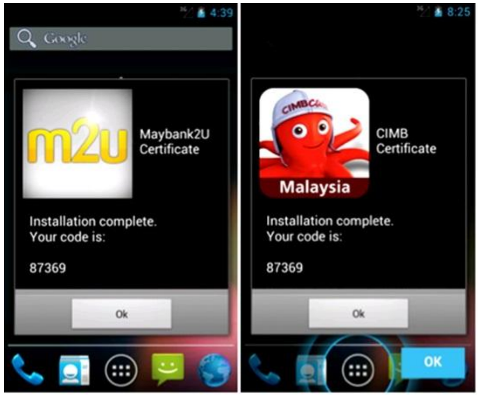
www.malaysiaedition.net/skimming-devices-found-in-four-genting-highlands-atms/

Published On: Thu, Aug 14th, 2014

National | By **henok**

Skimming devices found in four Genting Highlands ATMs

Banking Malware



Maybank2U Certificate

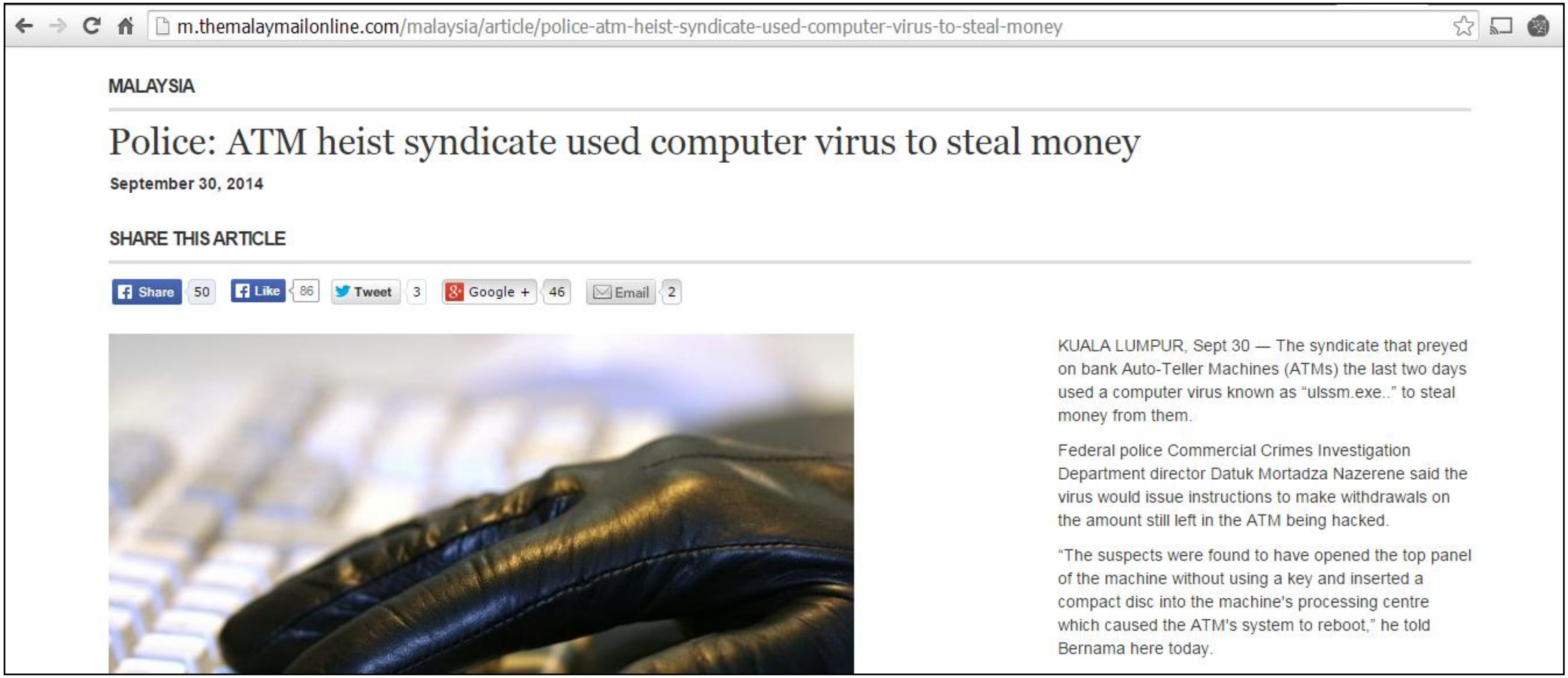
Installation complete.
Your code is:

87369

CIMB Certificate

Installation complete.
Your code is:

87369



m.themalaymailonline.com/malaysia/article/police-atm-heist-syndicate-used-computer-virus-to-steal-money

MALAYSIA

Police: ATM heist syndicate used computer virus to steal money

September 30, 2014

SHARE THIS ARTICLE

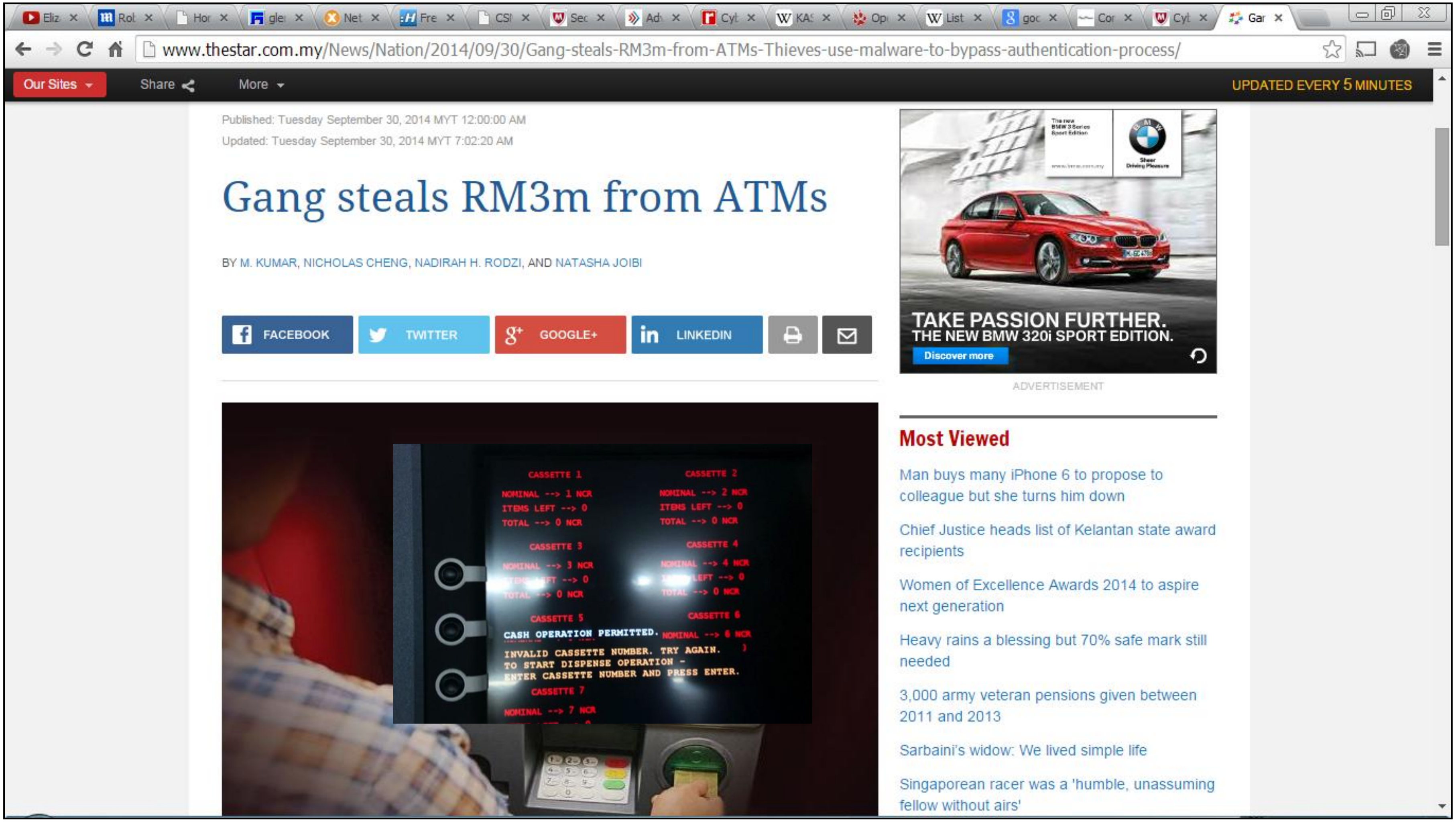
KUALA LUMPUR, Sept 30 — The syndicate that preyed on bank Auto-Teller Machines (ATMs) the last two days used a computer virus known as "ulssm.exe.." to steal money from them.

Federal police Commercial Crimes Investigation Department director Datuk Mortadza Nazerene said the virus would issue instructions to make withdrawals on the amount still left in the ATM being hacked.

"The suspects were found to have opened the top panel of the machine without using a key and inserted a compact disc into the machine's processing centre which caused the ATM's system to reboot," he told Bernama here today.

Source: http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/1002/index.html

ATM Hacking



www.thestar.com.my/News/Nation/2014/09/30/Gang-steals-RM3m-from-ATMs-Thieves-use-malware-to-bypass-authentication-process/

Published: Tuesday September 30, 2014 MYT 12:00:00 AM
Updated: Tuesday September 30, 2014 MYT 7:02:20 AM

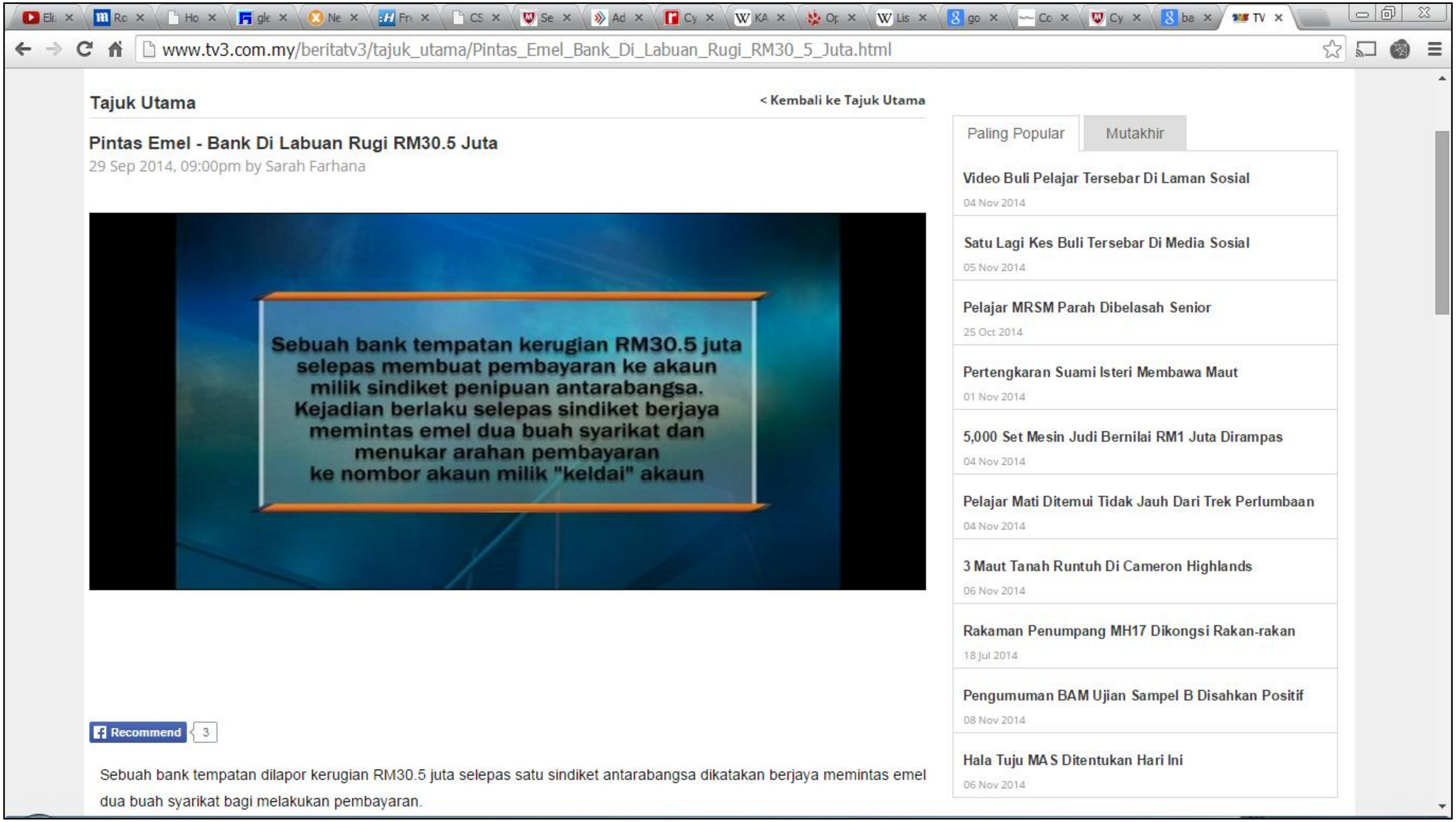
Gang steals RM3m from ATMs

BY M. KUMAR, NICHOLAS CHENG, NADIRAH H. RODZI, AND NATASHA JOIBI

Most Viewed

- Man buys many iPhone 6 to propose to colleague but she turns him down
- Chief Justice heads list of Kelantan state award recipients
- Women of Excellence Awards 2014 to aspire next generation
- Heavy rains a blessing but 70% safe mark still needed
- 3,000 army veteran pensions given between 2011 and 2013
- Sarbaini's widow: We lived simple life
- Singaporean racer was a 'humble, unassuming fellow without airs'

Email Interception



www.tv3.com.my/beritatv3/tajuk_utama/Pintas_Emel_Bank_Di_Labuan_Rugi_RM30_5_Juta.html

Tajuk Utama

< Kembali ke Tajuk Utama

Pintas Emel - Bank Di Labuan Rugi RM30.5 Juta

29 Sep 2014, 09:00pm by Sarah Farhana

Sebuah bank tempatan kerugian RM30.5 juta selepas membuat pembayaran ke akaun milik sindiket penipuan antarabangsa. Kejadian berlaku selepas sindiket berjaya memintas emel dua buah syarikat dan menukar arahan pembayaran ke nombor akaun milik "keldai" akaun

Recommend 3

Sebuah bank tempatan dilapor kerugian RM30.5 juta selepas satu sindiket antarabangsa dikatakan berjaya memintas emel dua buah syarikat bagi melakukan pembayaran.

Paling Popular | Mutakhir

Video Buli Pelajar Tersebar Di Laman Sosial
04 Nov 2014

Satu Lagi Kes Buli Tersebar Di Media Sosial
05 Nov 2014

Pelajar MRSM Parah Dibelasah Senior
25 Oct 2014

Pertengkaran Suami Isteri Membawa Maut
01 Nov 2014

5,000 Set Mesin Judi Bernilai RM1 Juta Dirampas
04 Nov 2014

Pelajar Mati Ditemui Tidak Jauh Dari Trek Perlumbaan
04 Nov 2014

3 Maut Tanah Runtuh Di Cameron Highlands
06 Nov 2014

Rakaman Penumpang MH17 Dikongsi Rakan-rakan
18 Jul 2014

Pengumuman BAM Ujian Sampel B Disahkan Positif
08 Nov 2014

Hala Tuju MAS Ditentukan Hari Ini
06 Nov 2014

IMPACT

FUTURE ATTACK??

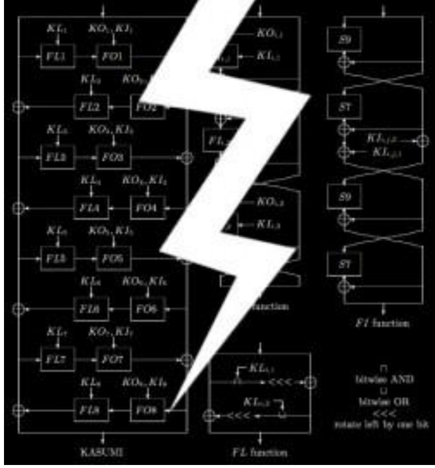
“Hackers”

“Hackers”

http://www.telegraph.co.uk/technology/news/11220524/Chinese-hacker-installs-Windows-98-on-an-iPhone-6.html

“Future” Attacks

- NFC
- RFID



“Future” Attacks

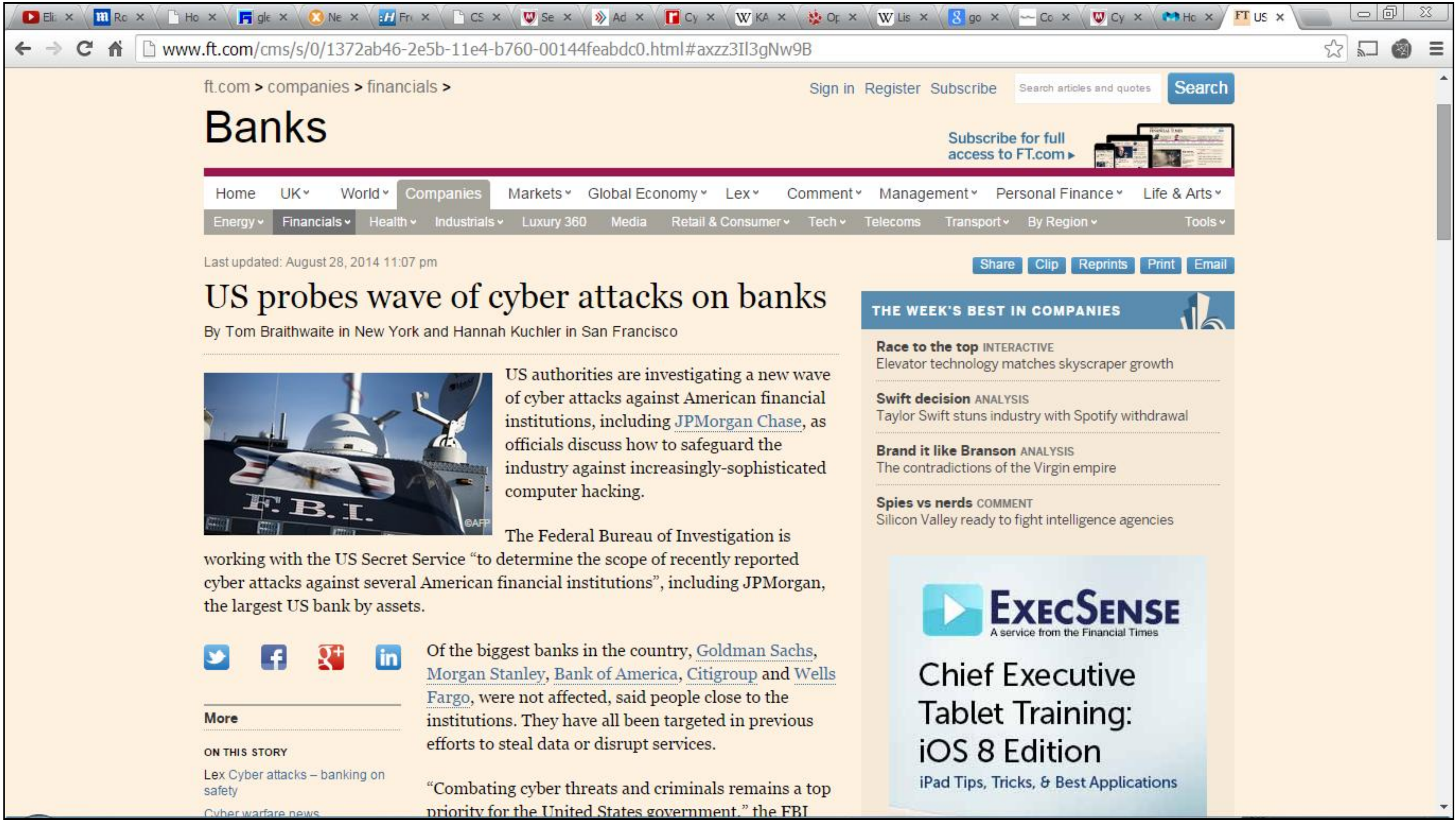
- Infrastructure attacks
- Real life crypto attack
  - 3G networks / Kasumi
- MiTM attack
  - Imitate base station
  - Femto cell
- Software Defined Radio (SDR)
  - Hacking satellite, Tetra etc

Financial Malware

- Common credential-stealing techniques such as form grabbing and HTML injection compatible with the major browsers (Internet Explorer, Firefox and Chrome);
- 32- and 64-bit ring3 (user-mode) rootkit capable of also "defending from other Trojans";
- Antivirus bypassing;
- Malware-to-C&C communication encryption;
- Sandbox bypassing.
- Price: USD 7,000.00!!

Source: http://securityintelligence.com/the-father-of-zeus-kronos-malware-discovered/#.VGIEQ_mUeSo

“Future” Attack



www.ft.com/cms/s/0/1372ab46-2e5b-11e4-b760-00144feabdc0.html#axzz3Il3gNw9B
ft.com > companies > financials >
Sign in Register Subscribe
Search articles and quotes
Search
Subscribe for full access to FT.com ▸
Home UK World Companies Markets Global Economy Lex Comment Management Personal Finance Life & Arts
Energy Financials Health Industrials Luxury 360 Media Retail & Consumer Tech Telecoms Transport By Region Tools
Share Clip Reprints Print Email
©AFP

Banks

Last updated: August 28, 2014 11:07 pm

US probes wave of cyber attacks on banks

By Tom Braithwaite in New York and Hannah Kuchler in San Francisco

US authorities are investigating a new wave of cyber attacks against American financial institutions, including JPMorgan Chase, as officials discuss how to safeguard the industry against increasingly-sophisticated computer hacking.

The Federal Bureau of Investigation is working with the US Secret Service “to determine the scope of recently reported cyber attacks against several American financial institutions”, including JPMorgan, the largest US bank by assets.

Of the biggest banks in the country, Goldman Sachs, Morgan Stanley, Bank of America, Citigroup and Wells Fargo, were not affected, said people close to the institutions. They have all been targeted in previous efforts to steal data or disrupt services.

“Combating cyber threats and criminals remains a top priority for the United States government,” the FBI

More

ON THIS STORY

Lex Cyber attacks – banking on safety

Cyber warfare news

THE WEEK’S BEST IN COMPANIES

Race to the top INTERACTIVE
Elevator technology matches skyscraper growth

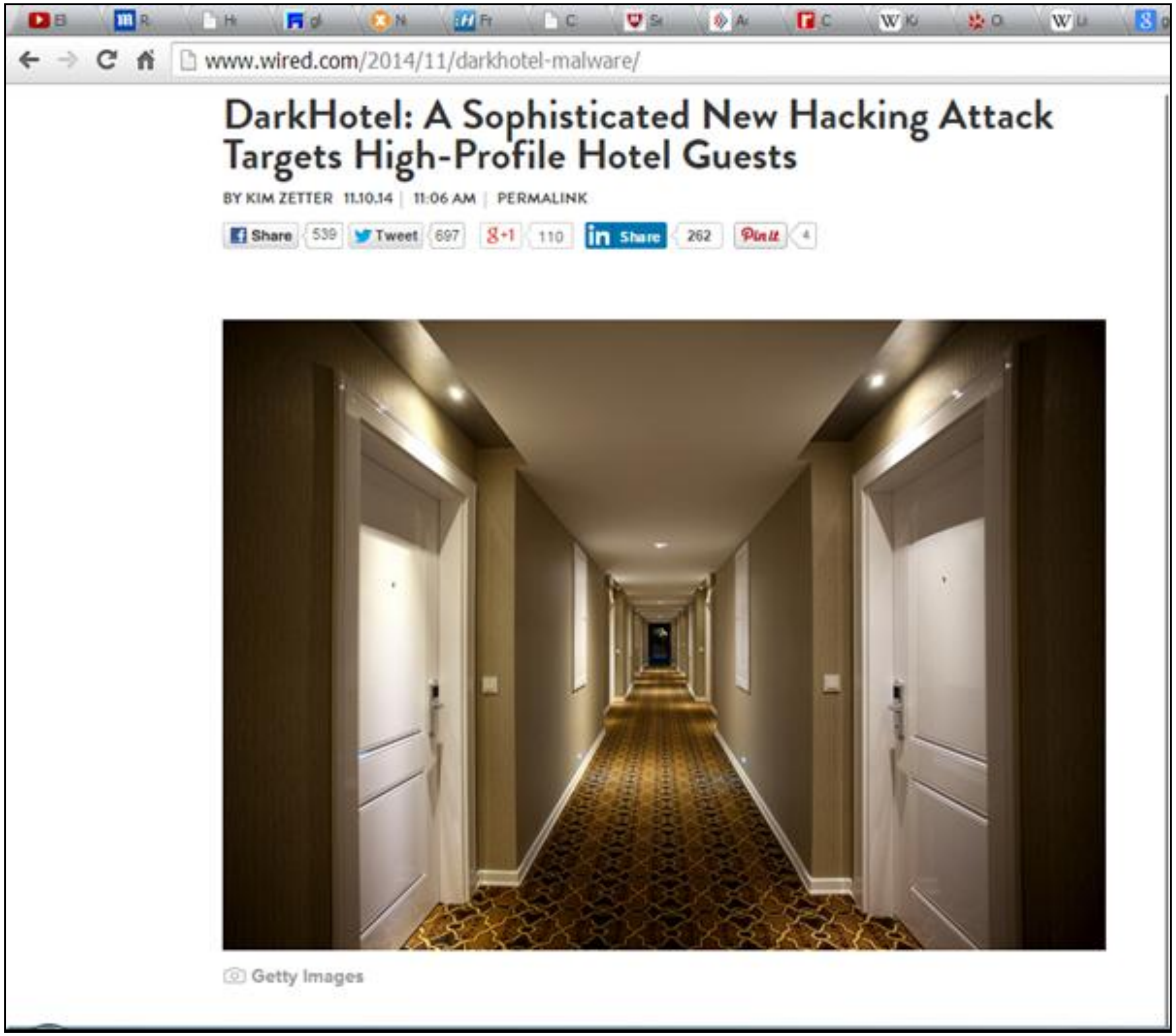
Swift decision ANALYSIS
Taylor Swift stuns industry with Spotify withdrawal

Brand it like Branson ANALYSIS
The contradictions of the Virgin empire

Spies vs nerds COMMENT
Silicon Valley ready to fight intelligence agencies

DarkHotel

“This Is NSA-Level Infection Mechanism”



www.wired.com/2014/11/darkhotel-malware/

DarkHotel: A Sophisticated New Hacking Attack Targets High-Profile Hotel Guests

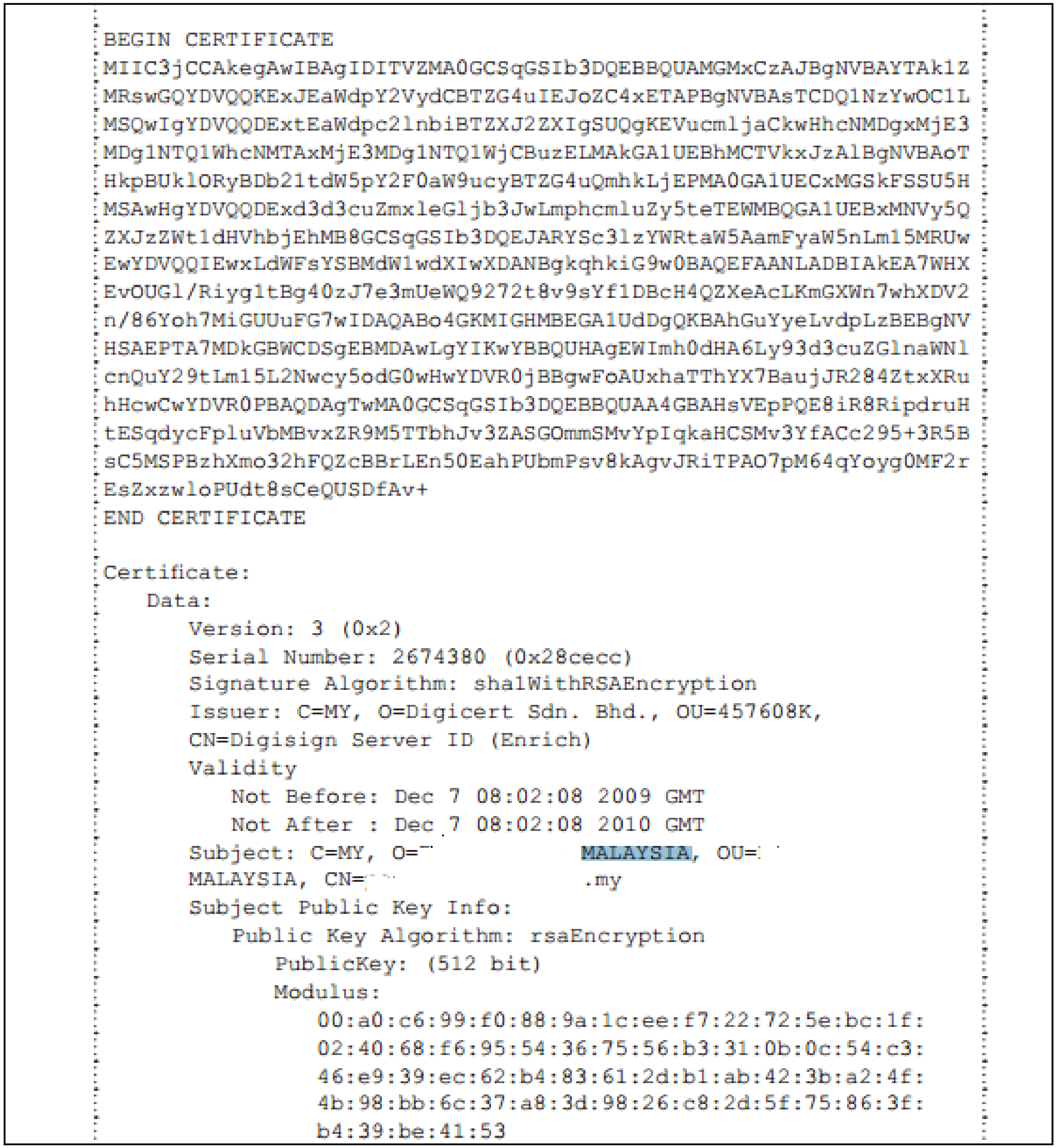
BY KIM ZETTER 11.10.14 | 11:06 AM | PERMALINK

Getty Images

- **Kaspersky Lab**
- **Spear Phishing**
- **200 C&C**
- **Kernel mode keylogger**
- **Digital certificate**
- **Active at least for 7 years**

Source: https://securelist.com/blog/research/66779/the-darkhotel-apt/

DarkHotel

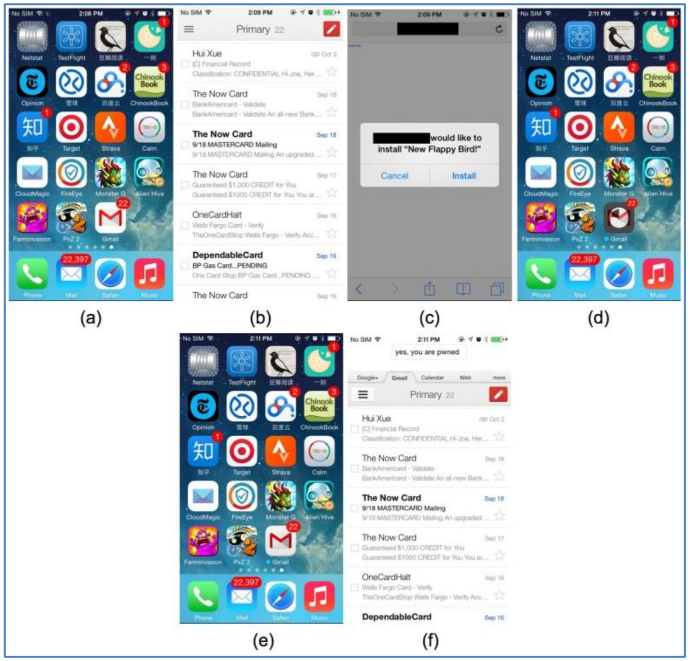


```
BEGIN CERTIFICATE
MIIC3jCCAkegAwIBAgIDITVZMA0GCSqGSIb3DQEBBQUAMGMxCzAJBgNVBAYTAk1Z
MRswGQYDVQQKExJEaWdpY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCDQ1NzYwOC1L
MSQwIgYDVQQDExtEaWdpc2lnbiBTZXJ2ZXIgSUQgKEVucmljaCkwHhcNMDgxMjE3
MDg1NTQ1WhcNMTAxMjE3MDg1NTQ1WjCBuzELMAkGA1UEBhMCTVkxJzAlBgNVBAoT
HkpBUklORyBDb21tdW5pY2F0aW9ucyBTZG4uQmhkLjEPMA0GA1UECxMGSkFSSU5H
MSAwHgYDVQQDExd3d3cuZmxleGljb3JwLmphcmluZy5teTEWMBQGA1UEBxMNVy5Q
ZXJzZWt1dHVhbjEhMB8GCSqGSIb3DQEJARYSc3lzYWRtaW5AamFyaW5nLm15MRUw
EwYDVQQIEwxLdWFsYSBMdW1wdXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEA7WHX
EvOUGl/Riyg1tBg40zJ7e3mUeWQ9272t8v9sYf1DBcH4QZXeAcLKmGXWn7whXDV2
n/86Yoh7MiGUUuFG7wIDAQABo4GKMIGHMBEGA1UdDgQKBAhGuYyeLvdpLzBEBgNV
HSAEPTA7MDkGBWCDSgEBMDAwLgYIKwYBBQUHAgEWImh0dHA6Ly93d3cuZGlnaWNl
cnQuY29tLm15L2Nwcy5odG0wHwYDVR0jBBgwFoAUxhaTThYX7BaujJR284ZtxXRu
hHcwCwYDVR0PBAQDAgTwMA0GCSqGSIb3DQEBBQUAA4GBAHsVEpPQE8iR8RipdruH
tESqdycFpluVbMBvxZR9M5TTbhJv3ZASGOmmSMvYpIqkaHCSMv3YfACc295+3R5B
sC5MSPBzhXmo32hFQZcBBrLEn50EahPUbmPsv8kAgvJRiTPAO7pM64qYoyg0MF2r
EsZxzwloPUdt8sCeQUSDfAv+
END CERTIFICATE
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2674380 (0x28cecc)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608K,
        CN=Digisign Server ID (Enrich)
        Validity
            Not Before: Dec 7 08:02:08 2009 GMT
            Not After : Dec 7 08:02:08 2010 GMT
        Subject: C=MY, O=              MALAYSIA, OU=
        MALAYSIA, CN=                  .my
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                PublicKey: (512 bit)
                Modulus:
                    00:a0:c6:99:f0:88:9a:1c:ee:f7:22:72:5e:bc:1f:
                    02:40:68:f6:95:54:36:75:56:b3:31:0b:0c:54:c3:
                    46:e9:39:ec:62:b4:83:61:2d:b1:ab:42:3b:a2:4f:
                    4b:98:bb:6c:37:a8:3d:98:26:c8:2d:5f:75:86:3f:
                    b4:39:be:41:53
```

Example of one of the digital certificate stolen to sign the malware.

FireEye Masque Attack vs WireLurker



Primary 22

Hui Xue — Oct 2
[C] Financial Record
Classification: CONFIDENTIAL Hi Joe, Her...

The Now Card — Sep 18
BankAmericard - Validate
BankAmericard - Validate An all-new Bank...

The Now Card — Sep 18
9/18 MASTERCARD Mailing
9/18 MASTERCARD Mailing An upgraded ...

The Now Card — Sep 17
Guaranteed $1,000 CREDIT for You
Guaranteed $1000 CREDIT for You You ar...

OneCardHalt — Sep 16
Wells Fargo Card - Verify
TheOneCardStop Wells Fargo - Verify Acc...

DependableCard — Sep 16
BP Gas Card...PENDING
One Card Stop BP Gas Card...PENDING ...

The Now Card — Sep 16

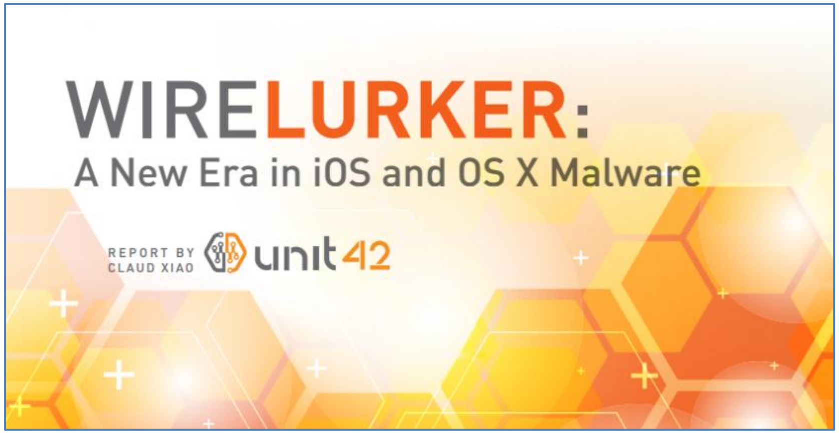
[redacted]

[redacted] would like to install "New Flappy Bird!"

Cancel | Install

yes, you are pwned

VS



WIRELURKER:

A New Era in iOS and OS X Malware

REPORT BY
CLAUD XIAO

unit 42

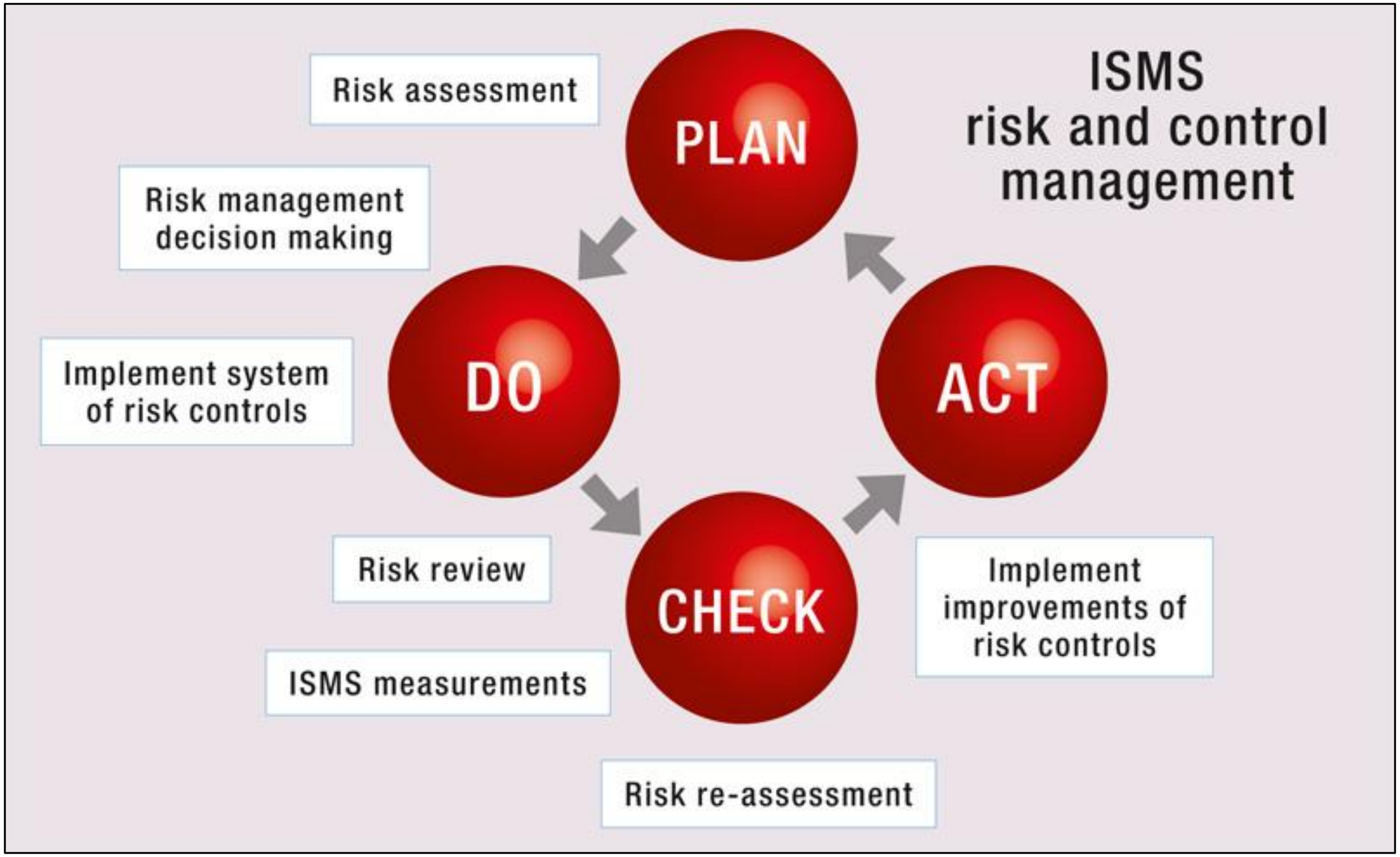
Source:
http://www.fireeye.com/blog/technical/cyber-exploits/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html
https://www.paloaltonetworks.com/content/dam/paloaltonetworks.com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

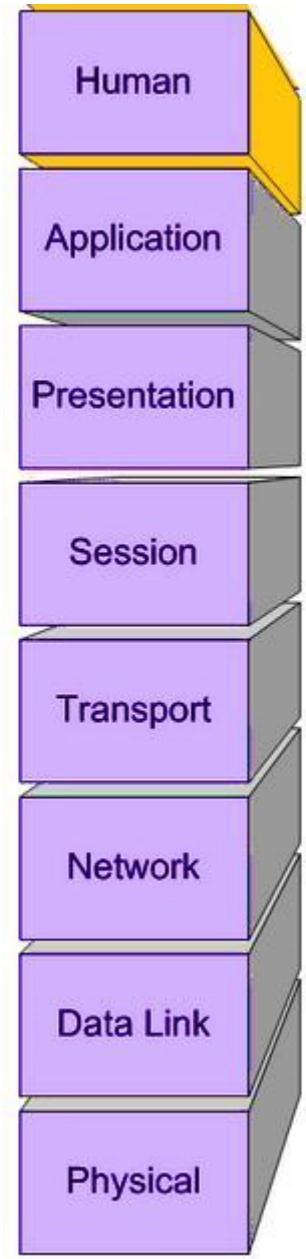
Conclusion

INNOVATION = $$$$$$$$

Conclusion

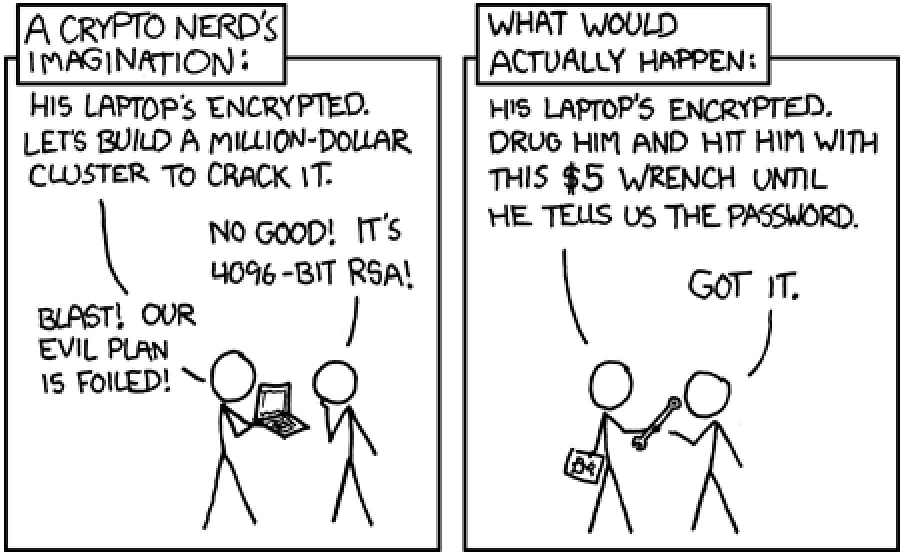
- Managing risks.





THIS MUST BE THE MOST IMPORTANT ELEMENT IN YOUR CYBER SECURITY STRATEGY AND PLANNING

CONCLUSION


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Source: http://xkcd.com/538/

CONCLUSION

csm-ace
CYBER SECURITY MALAYSIA
AWARDS, CONFERENCE &
EXHIBITION
2014

TERIMA KASIH